

Amendments to the Specification:

Please replace paragraph [0066] with the following amended paragraph:

[0066] The setup of dynamic authentication involves computing the expected in-memory page hashes of all read-only module pages. The page hashes are stored in tables for quick reference in subsequent page verification. The basis for establishing what the code pages should look like in memory is a signed disk image of the PE file itself or its corresponding prehash. Determining the expected page hash is complicated by the existence of relocations and import address tables. Authenticating relocated pages and import tables forces us to apply the logic used by the Windows WINDOWS™ operating system loader. For example, if the module being authenticated was rebased by the OS, we have to apply relocation fix-ups to the appropriate addresses before computing each page hash. If the module has static imports or delay imports, we have to mimic the loader when computing the expected import address table (IAT).